



National Aeronautics and  
Space Administration

**John C. Stennis Space Center**  
Stennis Space Center, MS 39529-6000

**SPD 2800.2 Basic**  
**November 2003**

## John C. Stennis Space Center SSC Information Technology Resources Usage Policy



Stennis Policy Directive	SPD 2800.2	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: November 7, 2003	
	Expiration Date: November 7, 2008	
Page 3 of 6		
Responsible Office: RA00/Center Operations Directorate		
<b>SUBJECT: SSC Information Technology Resources Usage Policy</b>		

## 1. POLICY

a. Information Technology (IT) resources are provided for official business and only to the level sufficient and necessary to accomplish officially assigned government duties and responsibilities consistent with SSC, NASA, and Government established policy, procedures, and guidelines. Information Technology resources may not be used in any manner that is illegal, that would cause embarrassment to NASA or the federal government, or conflict with Government guidelines and policies.

b. Limited personal use of IT resources is authorized for activities that are reasonable and fall within the guidelines listed herein.

c. Limited personal use of telephonic resources, other than cellular telephones and cellular telephone capabilities within wireless Personal Digital Assistants, is authorized for activities that are reasonable and necessitate execution from the work place. Personal use of cellular telephones is not permitted. (See NPD 2540).

d. Also authorized are activities that serve a legitimate public purpose such as enhancing professional skills, increasing employee proficiency in use of the equipment, or allowing the employee to stay near his/her desk.

e. In order to ensure that personal use does not adversely affect the performance of official duties, authorized personal use is subject to the following guidelines:

(1) Whenever possible, personal use should be limited to before or after work hours or during lunch or other authorized breaks.

(2) Personal communications should not overburden computer network, communications, or other IT systems.

(3) Authorized personal use must be infrequent and short.

(4) Unless noted in other policy, procedures, or guidelines, employees are prohibited from any personal use of IT resources that results in additional charges to the Government. It is the employee's responsibility to be aware if cost is involved. Employees may be subject to disciplinary action and will be required to reimburse the Government for cost incurred including any administrative costs. In the case of cellular telephones, the employee will be responsible for reimbursing the government at the "Out of Plan" per minute peak rate for all outgoing and incoming minutes for personal calls. The minutes will be fractional or whole as tracked by the cell carrier. If the plan provides "no cost" minutes for calls, the employee will be required to reimburse the government at the peak per minute rate. This is in addition to administrative costs and possible disciplinary actions.

Stennis Policy Directive	SPD 2800.2	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: November 7, 2003	
	Expiration Date: November 7, 2008	
Page 4 of 6		
Responsible Office: RA00/Center Operations Directorate		
<b>SUBJECT: SSC Information Technology Resources Usage Policy</b>		

(5) Personal communications to solicit business, advertise, or engage in other activities in support of an employee's private business enterprise are strictly prohibited. Any activity that would reflect negatively on NASA (e.g., harassing e-mail, electronic chain letters, calling sexually related numbers, surfing sexually oriented websites, or downloading sexually explicit pictures) is also prohibited.

(6) Use of IT resources for professional development is permitted.

f. Since IT resources are provided to support the work of the Center, there should be no expectation of personal privacy. IT resources may be reviewed by managers, supervisors, and other authorized individuals at any time. Usage of IT resources may be monitored according to Government policy and periodically examined only by authorized personnel for security and policy compliance purposes. Supervisors may issue more restrictive guidance if deemed appropriate.

g. The following definitions apply to this policy:

(1) Information Technology Resource – Electronic devices, both Government owned and leased, used for the storage and/or transmission of information including computers, networks, telephones, wireless services, FAX machines and other information transfer devices.

(2) Official Business – The work necessary for direct performance of assigned duties and tasks.

(3) SSC Employee – All employees at SSC to include but not limited to part time, full time, temporary, TDY, visiting professors, and students.

## 2. APPLICABILITY

This policy applies to all NASA and SSC contractor support personnel using NASA IT resources.

## 3. AUTHORITY

- a. 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended.
- b. OMB Circular A-130, Management of Federal Information Resources.
- c. 40 U.S.C 1401, et. seq., Information Technology Management Reform Act of 1996.

## 4. REFERENCES

All references are assumed to be the latest version unless otherwise specified.

- a. NPD 2810.1, Security of Information Technology.
- b. NPG 2810.1 Security of Information Technology.
- c. NPD 2540.1, Use of Government Telephones.

Stennis Policy Directive	SPD 2800.2	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: November 7, 2003	
	Expiration Date: November 7, 2008	
Page 5 of 6		
Responsible Office: RA00/Center Operations Directorate		
<b>SUBJECT: SSC Information Technology Resources Usage Policy</b>		

d. NPD 2800.1, Managing Information Technology.

## 5. RESPONSIBILITY

a. SSC employees are responsible for their individual official and unofficial use of IT resources consistent with this SPD, and for the reimbursement to the government of all government incurred costs associated with their unauthorized use of IT resources. SSC employees are further responsible for reimbursement of personal calls on cellular telephones as designated in Section 1.e (4).

b. Supervisors are responsible for usage management of IT resources within their jurisdiction. Such responsibility includes authorizing personal use as permitted within this SPD or as necessary in the interest of the Government and identifying for collection and potential disciplinary action all unauthorized IT resource usage within their jurisdiction.

c. The SSC IT Security Manager and SSC Telecommunications Manager will establish procedures to monitor IT resource usage, to detect unauthorized IT resource usage that constitutes a threat to the interests of the Government, to mitigate the effects of unauthorized IT usage on the Government, and to preserve all evidence in the event of the discovery of potentially criminal activity. These procedures will include steps for reporting to the NASA Inspector General, SSC Chief, Information Management Division and SSC Chief Information Officer all instances of actual or suspected criminal use of IT resources, and/or other misuses of IT resources which negatively impact the performance of the Government at SSC.

d. The SSC IT Security Manager will authorize the blocking of specific Internet web sites and/or categories of Internet web sites by functional description that are determined by committee to be inappropriate for access within the SSC workplace.

e. The SSC Network Operations Manager will implement procedures for the monitoring and restriction of access to Internet web sites determined by the SSC IT Security Manager to be inappropriate for access within the SSC workplace.

f. The SSC Telecommunications Manager will implement procedures for the restriction of access to telephone sites determined to be inappropriate for access within the SSC workplace. The procedures will also include steps for obtaining supervisor certification that toll calls under their jurisdiction are for official business or are authorized personal calls.

g. The Chief, Information Management Division will assure provisions of this SPD are implemented and maintain and report metrics associated with this SPD. The Chief, Information Management Division is also responsible for resolution of any questions or issues that arise concerning usage of IT resources.

Stennis Policy Directive	SPD 2800.2	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: November 7, 2003	
	Expiration Date: November 7, 2008	
Page 6 of 6		
Responsible Office: RA00/Center Operations Directorate		
<b>SUBJECT: SSC Information Technology Resources Usage Policy</b>		

## 6. MEASUREMENTS

The following performance measures will be collected and maintained by the Chief, Information Management Division:

- a. Number of reported instances of criminal or other unauthorized use of IT resources.
- b. Inventory of Internet web sites or web site functional categories to which SSC access is blocked or limited, and the number of times unauthorized attempts are made to contact these sites from SSC IT resources.
- c. Number of user IT resources monitored each month.

## 7. CANCELLATION

SPG 2800.1, SSC Information Technology Resources Usage Policy dated July 12, 1998.

*Signature on file*

Michael U. Rudolphi  
Interim Director

DISTRIBUTION  
SDL-5  
NODIS